Niko Pajunen

Overview of Maritime Cybersecurity

Bachelor's Thesis

Marine Technology

January 2017

Kaakkois-Suomen ammattikorkeakoulu

Tekijä	Tutkinto	Aika
Niko Pajunen	Merikapteeni	Tammikuu 2017

Opinnäytetyön nimi

Katsaus merenkulun kyberturvallisuuteen

47 sivua
3 liitesivua

Toimeksiantaja

Kaakkois-Suomen ammattikorkeakoulu

Ohjaaja

Yliopettaja Martti Kettunen

Tiivistelmä

Opinnäytetyön tarkoituksena oli kartoittaa kyberturvallisuuden tilaa merenkulussa. Päätavoitteena oli selvittää, millaisia tietoverkkoja aluksissa käytetään ja kuinka turvallisia ne ovat. Toisena tavoitteena oli selvittää suomalaisen päällystön tietoteknisen osaamisen taso sekä heidän ymmärryksensä tietoturvasta.

Työssä esitellään merenkulun tietotekniikkaan liittyvää lainsäädäntöä sekä ohjeistusta niin IMO:lta kuin luokituslaitoksilta. Lisäksi käydään läpi eri navigointilaitteiden haavoittuvuuksia erilaisten ulkoisten uhkien osalta ja esitellään laivalla olevien tietokoneiden vaikutusta laivan sisäverkon turvallisuuteen. Työssä esitellään merenkulkijoiden tietoteknisen koulutuksen tasoa suomalaisissa ammattikorkeakouluissa. Lisäksi käydään läpi, miten nykyiset vakuutukset kattavat aluksen tietoturvavahingot, miten automaatio on vaikuttanut järjestelmien turvallisuuteen sekä miten merenkulku tulee kehittymään tulevaisuudessa ja miten näihin muutoksiin tulisi varautua tietoturvan osalta. Työssä perehdytään myös erilaisiin hyökkäyskeinoihin.

Työssä tutkittiin kahden suomalaisen laivan tietoverkon rakennetta. Opinnäytetyössä esitellään, miten eri laitteet on kytketty verkkoon ja mitä toimenpiteitä on tehty kyberturvallisuuden parantamiseksi. Työssä esitellään myös mahdollinen hyökkäysskenaario toisen laivan verkkoon. Suomalaisen päällystön osaamista tutkittiin 26 kysymyksestä koostuvalla kyselyllä, johon vastasi yhteensä 17 henkilöä. Kyselyn analysointi jaettiin kolmeen osa-alueeseen: taustat, IT-osaaminen ja kyberturvallisuustietoisuus.

Tutkimus jäi osittain vajaaksi, sillä tutkittujen alusten kytkinten ja palomuurien konfigurointia ei päästy tarkastelemaan. Aihe vaatisi lisäselvitystä. Yleisellä tasolla laivojen verkoilla on potentiaalia olla turvallisia, mutta kehitettävää on. Päällystön osaaminen ylitti alkuperäiset odotukset monin osin, mutta vakaviakin puutteita löydettiin. Tulevaisuudessa olisi järkevää ottaa kyberturvallisuuskoulutus osaksi merenkulkijoiden osaamista. Lisäksi esitellään konsepti IT-perämiehestä: mitä hänen koulutukseensa, osaamiseensa ja vastuihinsa kuuluisi.

Asiasanat

kyberturvallisuus, haavoittuvuudet, laivojen tietoverkot, inhimillinen tekijä

Author	Degree	Time
Niko Pajunen	Bachelor of Marine Technology	January 2017

Thesis Title

Overview of Maritime Cybersecurity

47 pages
3 pages of appendices

Commissioned by

South-Eastern Finland University of Applied Sciences

Supervisor

Martti Kettunen, Principal Lecturer

Abstract

The purpose of this thesis was to find out the state of cybersecurity in shipping. The main objective was to study what sort of networks are used onboard vessels and how secure they are. The second objective was to study Finnish officers' IT skills and security awareness.

Maritime IT legislation and guidelines from the IMO and classification societies are presented in this thesis. The vulnerabilities of various navigation devices are listed. The effect of onboard computers on vessel's network are presented. IT education of seafarers in Finnish universities was investigated. The insurance coverages concerning cyberattacks, effect of automation on system security and the future development of maritime sector on cybersecurity were studied. Theory of both remote side and client side cyberthreats was researched.

Network structures of two Finnish vessels were investigated for this thesis. The different devices in the network and IT practices of vessels are presented. A possible attack scenario against the first vessel's network is described. Finnish officers' IT skills were studied using a survey consisting of 26 questions. There was a total of 17 answers. The results were analysed in three categories: backgrounds, IT skills and security awareness.

This thesis is partially incomplete as it was not possible to study the configurations of the vessels' switches and firewalls. This subject should be studied further in the future. In general, the existing networks have potential to be secure but there is still room for improvement. The IT skills of the officers were better than initially expected but there were also some serious deficiencies. Training seafarers on cybersecurity should be made essential in the future. In addition, a concept of IT officer was considered in terms of education, skills and responsibilities.

Keywords

cybersecurity, vulnerabilities, vessels' networks, human factor

TABLE OF CONTENTS

ABBREVIATIONS AND TERMS

Active Directory	A service that authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software.
AIS	Automatic Identification System. It is designed to be capable of providing information about the ship to other ships and to coastal authorities automatically via VHF radio frequency.
AMOS	A maintenance software commonly used on board.
DHCP	Dynamic Host Configuration Protocol. A service that distributes network configuration parameters to domain computers.
Domain	A group of computers that function and are administered as a unit and are identified by sharing the same domain name on the the internet.
ECDIS	Electronic Chart and Display Information System. Electrical aid to navigation which complies with IMO regulations.
IMO	International Maritime Organization. A specialized organization of the United Nations regulating shipping.
Man-in-the-middle	A method where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
ISPS	International Ship and Port Facility Security Code. An amendment of SOLAS which states the minimum security arrangements for ports and ships.

Port	A software based construct that identifies certain type of traffic. For example, port number 80 is used by web browsers.
SMS	Safety Management System. An organized system planned and implemented by the shipping companies to ensure safety of the ship and marine environment. It details all the important policies, practices, and procedures that are to be followed to ensure safe functioning of ships at the sea.
SOLAS	Safety of Life at Sea. A convention that regulates minimum safety standards in construction, equipment and operation of vessels.
STCW	Standards of Training, Certification and Watchkeeping for Seafarers. A code that sets qualification standards for maritime personnel.
UKHO	United Kingdom Hydrographic Office. An institute that collects hydrographic geospatial data to protect lives at sea.
VLAN	Virtual Local Area Network. A VLAN might comprise a subset of the ports on a single switch or subsets of ports on multiple switches. By default, systems on one VLAN do not see the traffic associated with systems on other VLANs on the same network.
VPN	Virtual Private Network. A secure connection that extends private network over the internet.

1 INTRODUCTION

Overall, technology has developed at an astonishing speed during last decades. However, shipping as an industry has always been a little slow as every invention or device needs to be approved by the IMO and the classification societies. A good example of maritime sector's slowness is the implementation of the ISPS code. It received its start from the 9/11 attacks after which the US officials demanded improvement for security on ships and at ports. The code came into force in July 2004. It took almost three years to create and implement a new code and this was the fastest implementation in IMO's history.

This slowness to react can be understood when one starts to think about digitalization on board. Only now ECDIS is becoming mandatory for all vessels even though it was approved for navigation in November 1995. However, it is not all bad as more and more material is being transformed into digital format. Good example of this are the navigation manuals such as List of Radio Signals and List of Lights. However, there is a down side: it is not possible to access these files should a blackout occur since the computers are not usually behind an uninterruptible power source.

The importance of cybersecurity has always been acknowledged but in recent years it has risen to a whole new level. Yet it is rather easy to neglect cybersecurity even with small actions. Integrity and security of systems is particularly important for vessel as there are vast amounts of money involved.

This thesis includes a theoretical part where vulnerabilities of different onboard navigational devices will be explained. The current security situation and visions for the future will be discussed. Different cyberthreats are explained on a more technical basis.

One could roughly separate maritime cybersecurity into two aspects: the structure and security of the vessel's network and the human factor. These aspects will be studied in this thesis. The networks of two vessels were studied and evaluated. In addition, the vessels' IT practises are discussed. The human factor was studied using a survey. The questions concerned deck and engine officers' IT backgrounds, IT skills and security awareness.

The author of this thesis has a degree in Computer Sciences from a vocational college and experience working as an IT support. This gives the author proficient understanding for evaluating IT related topics.

2 CYBERSECURITY IN SHIPPING

2.1 Introduction to onboard cybersecurity

Cybersecurity is rather large and complex concept and it is somewhat new in the field of shipping. Rules and regulations are an important part of maritime industry so we will take a look at the legislation concerning cybersecurity. Additionally, we study the weaknesses of electronic aids to navigation including ECDIS, AIS and GPS. Bridge integration and the effect of onboard computers on the network of a vessel will conclude this chapter.

2.1.1 Legislation and guidelines

The IMO published a new circular no. 1526 Interim Guidelines on Maritime Cyber Risk Management on June 2016. The document states that cyber threats are real and something should be done to prevent them (IMO 2016, 1). However, there are no mention about concrete actions how to achieve this.
It is only mentioned that there should be distinction between information technology and operational technology system (IMO 2016, 2).
My interpretation of this is that, for example, loading computers should be completely separated from the internet. All in all, the document is full of empty phrases and what makes it even worse is that it is only recommendable and not mandatory. With this the IMO shifts the responsibility from themselves to shipping companies and IT systems' suppliers.

It is disappointing that this is what they came up with. Computers have been essential tools on board for years now and the IMO is still incapable to deliver proper guidelines for cybersecurity. It must be admitted that vessels are diverse and it might be difficult to give instructions that could be easily applied to all vessels.

Shipping companies should have procedures and guidelines regarding cybersecurity. The latest edition of Bridge Procedures Guide (2016, 59) states the following: *The exchange of electronic data between ships and shore authorities, service providers, charterers and owners/operators has increased significantly over recent years. The use of electronic data exchange, including updates to navigational systems and software, exposes users to the possibility of unauthorized or malicious access. This creates a risk to the safety and security of shipboard systems.*

To protect commercial interests, as well as to ensure that safety and environmental protection are not compromised, it is important that seafarers comply with Company cybersecurity procedures. Company procedures should consider industry guidelines as well as any regulatory requirements addressing cybersecurity.

This is terribly vague description of cybersecurity and it gives no recommendations to the companies. This is peculiar as Bridge Procedures Guide usually gives very specific guidelines, recommendations and even ready checklists. The previous edition from 2007 did not even mention cybersecurity. This shows that maritime industry hasn't been able to adopt to potential threats of technology it has already adapted.

From my personal experience, some companies have mentioned cybersecurity in their Safety Management System, but once again, there have been only vague mentions about basics of cybersecurity and not any direct actions to be taken or guidelines.

Classification societies have a large role on developing safe and secure ways of work. Lloyd's Register has recognised the importance of cybersecurity and published guidelines on February 2016. This is a rather extensive document dealing with different areas of ICT including cyber security. It also recognises that cybersecurity related education should be given to all related crew members. (Lloyd's Register 2016, 8)

Ships do not usually have the luxury of 50+Mb broadband: many share a single 64Kb Inmarsat connection between a number of onboard systems. This means that in the event of attack or infection, any files required to rebuild or repair an onboard PC-based system must be on the ship already, rather than

having to be downloaded (something that could take a day using Inmarsat). Most vessels currently do not have operating system disks on board, let alone proprietary software, drivers or patches. This connectivity constraint also provides a single point of failure and vulnerability. These significant issues have to be addressed during the system's design. (Lloyd's Register 2016, 9)

It is also acknowledged that ICT systems should not be acquired for the sake of technology but to serve crew in their tasks (Lloyd's Register 2016, 5). The document gives guidelines for multiple fields of ICT but admits that giving prescriptive rules is not possible (Lloyd's Register 2016, 10).

2.1.2 ECDIS

ECDIS has become an important aid for navigation. It is essential for all new vessels and it will become mandatory for existing vessels in July 2018. ECDIS is basically a Windows based computer with navigation software installed on it. The following table shows specifications of the hardware in Consilium's system and they can be reviewed in full in Appendix 2.

Table 1. Consilium ECDIS specifications

Display	19" 1280x1024, 23" 1600x1200 or 27" 1920x1200
Processor	Intel Core 2 Duo 2,26 GHz
RAM	2 Gb 800 MHz DDR2
Graphics Card	Intel 4500MHD Integrated
Hard Disk	30 Gb SSD
Operating system	Windows XP Professional Service Pack 2

As can be seen from Table 1, the computer running ECDIS is completely obsolete. In my experience, the computers are barely capable of running the ECDIS software. There are long waiting times when loading a new route. The worst part is that all systems that I have seen are running Windows XP. Tim Rains, Security Director from Microsoft, explains that the worst part is that Windows XP will basically have "zero day" vulnerability forever as it no longer

receives security updates (Rains 2013). One saving fact is that ECDIS is not usually connected to the internet and therefore cannot be infected remotely. The risk is when an officer installs updates to the system. This will be dealt more profoundly in chapters 3.1 and 3.2.

Another aspect is that the computers running ECDIS are completely unprotected. There are no antivirus (AV) software installed on them. One reason is that the computers simply do not have enough computing power to run them beside the navigation software. The second point is that some AV software no longer support Windows XP.

The NCC Group conducted a survey regarding ECDIS's vulnerabilities. The test environment included an ECDIS demo from one of the major manufacturers ran on Windows 7 (32-bit) with basic configurations and no firewall or AV software were installed. Firstly, they were able to browse, list and download any files stored on the computer. Secondly, they could upload, delete or replace any file on the ECDIS Windows 7 system. Other vulnerabilities were also found. (NCC Group 2014, 8)

2.1.3 AIS

AIS has been mandatory on all passenger vessels and international sea-going vessels with 300GT or more since 2002 (Balduzzi, Wilhoit & Pasta 2014, 3). It has made navigation safer especially in limited visibility conditions. However, AIS has no built-in security measures, making it vulnerable to external threats. It has been proved that it is possible to disable AIS communication, tamper with existing AIS data, trigger SAR alerts and spoof collisions (Balduzzi et al. 2014, 3). However, all these threats can be avoided by comparing data to other sources such as radar and visual look-out.

2.1.4 GPS

GPS is an essential device for determining the ship's position at open sea. The only alternative is astronomical navigation. GPS feeds position information for many navigational systems, allowing them to work properly. In 2013, Todd Humphreys and his students from University of Texas conducted

a test to spoof ship's GPS system. They were able to replace genuine GPS signals with fake signals sent by a 2000 $ spoofer causing navigation equipment to think that the ship is three degrees off course (Psiaki & Humphreys 2016). The worst part is that the GPS device cannot tell whether it is being spoofed or not.

The same people behind the proof of concept worked on countermeasures. As genuine GPS signals come from various satellites in different directions, a spoofing signal will most likely come from a single source. They were able to use this fact in their defensive device, which could tell if the signal was spoofed with a six second delay. (Psiaki & Humphreys 2016)

Earlier this year, GPS manufacturer U-blox released the first commercially available spoofing defence for consumer GPS receivers in a firmware update to its M8 line of navigation systems (Psiaki & Humphreys 2016).

2.1.5 Integrated Bridge

The first forms of bridge integration are from late 1960. As computers of that time were not that advanced, the interfacing between devices was done using analogue connections such as synchro transmitters and receivers, stepper transmitter and stepper receiver, pulses and analogue DC voltage. Today, navigation equipment is connected using serial cables in accordance with Marine Industry Standard Serial Data Communication IEC61162. This way all devices are compatible with each other. However, analogue information is still used for devices as propeller pitch or rudder angle indicators (HiMarine 2016, 82).

Some years ago, it was common practice to buy each navigation device separately. If one was not careful enough it was possible that two devices weren't compatible with each other. Today's bridges are more or less integrated which means that shipping company orders the bridge equipment from one manufacturer which provides all the devices and ensures compatibility. Example of Furuno's integrated bridge can be seen in Figure 1. Acquiring the bridge equipment as a package from one manufacturer also clears up responsibility questions.

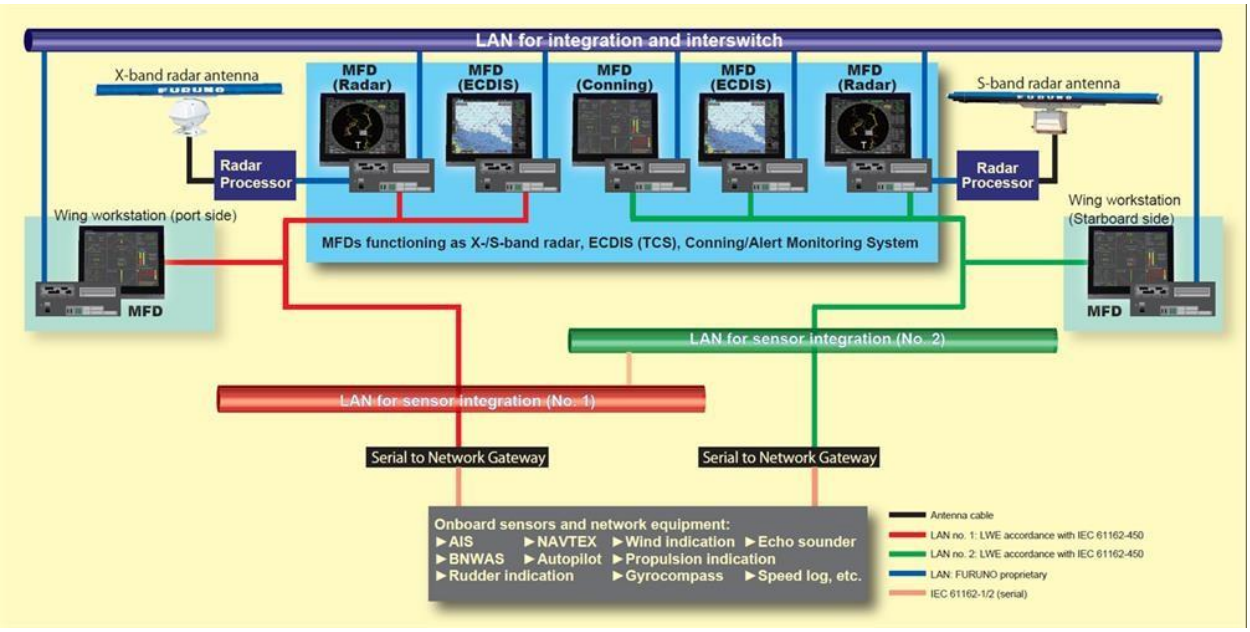


Figure 1 Furuno's integrated bridge (Furuno https://www.furuno.fi/fin/ulkomaanliikenne/navigointijarjestelmat/integroidut_komentosillat/)

Radar, ECDIS and conning displays receive information from many input devices. As mentioned earlier, this data is transferred using serial cables. There has been some development with the interface as some devices are connected using Ethernet cables.

There has been talk that in the future all navigational devices could be connected to a single local area network. This would make cabling easier but there are some security issues. As ECDIS is connected to the internet it would indirectly connect the whole navigation network to the internet. This would lead to a need for security measures, for example, to prevent unauthorised access to gyro compass. There is always a possibility to gain access to devices connected using Ethernet cables. This possibility exists for serial cables too but it is far more unlikely to happen.

2.1.6 Onboard computers

Computers are used for various tasks on board vessels. The most important functions are calculating the vessel's stability, monitoring sensor data, updating ECDIS and general information exchange with the company and shore-based officials. Some of the computers are connected to the internet continuously and this makes them vulnerable to cyber threats. Usually the

computers used for monitoring and controlling onboard machinery, such as the main engine, are not connect to the internet. *When designed properly, the use of ICT can increase efficiency and safety through improved monitoring and communication, and greater situational awareness on the bridge, in the engine room and in other operational areas* (Lloyd's Register 2016, 2).

One vulnerability is the crews' email addresses. They are almost in every case formed in the following way: jobtitle.shipname@shippingcompany.com. This makes phishing attempts effortless as one can guess the email address with ease. As Panda Security proved in their study 'Operation "Oil Tanker" The Phantom Menace', all it takes to infect computer is to open a PDF file. The file then extracts itself to multiple files and begins to gather and send credential information to the attacker (Panda Security 2015, 4). The smartest part is that the malware uses legitimate tools making it invisible to AV software (Panda Security 2015, 6).

Usually there are a few computers on board reserved for crew's personal use. Since they are available for everyone, one should take extra care when using these computers. Who knows what someone else might have done with these. Special attention should be taken when using USB devices as it is possible to infect other machines this way.

Once again, IMO's guidelines are disappointing. There are not really any regulations for computers used on board. The only reference is IMO's Circular MSC/Circ.891 Guidelines for the On-board Use and Application of Computers from 1998, which hasn't stood the test of time. At that time, computers were beginning to come on board and this was the IMO's response to clear things up. It might have been enough at the time, but it is not enough today. The problem is that the document is still valid since even the latest edition of SOLAS from 2014 still refers to this circular. Surprisingly in chapter 3.1.6 it is stated that *Computer-based systems should be protected against unintentional or unauthorized modification of programs and data* (IMO 1998, 3). However, means to achieve this are not presented nor are there any guidelines for this.

2.2 Situation at present and in future

This chapter takes a more general view on the topic of maritime cybersecurity. The education of Finnish officers in Finnish universities of applied sciences will be studied as well as insurance coverages concerning cybersecurity incidents. The future of shipping is also pondered as automation develops and autonomous vessels may become possible.

2.2.1 Education

Education is an essential part of becoming a professional seafarer. IMO's STCW code dictates what should be included in seafarers' education. The latest amendments came into force in 2012. However, the word 'cyber' is not mentioned even once in the code. Only the electro-technical officer is required to understand the following: *main features of data processing, construction and use of computer networks on ships, bridge-based, engine-room based and commercial computer use* (STCW 2011, 172). To make matters worse, most ships do not even have an electro-technical officer. Usually there is an electrician on board but even that is not necessary. In the worst case, there is no one who has the understanding of the ship's network.

Deck officers are only required to know how to use computer based radio equipment and to fix possible software related problems (STCW 2011, 320). There is no mention of anything computer training even though computers have been an essential part of shipping for years. Technically, using computers is not part of safe navigation and watchkeeping, but they are important tools.

Fortunately, things are little better here in South-Eastern Finland University of Applied Sciences. We have two IT related courses as part of our education. The first one is worth five credits and is focused on the use of Microsoft Office tools. The second one is worth three credits and is focused on the use of programs commonly used on board. Marine Engineers also have these courses. However, neither of these courses takes into account cybersecurity in any way.

IT studies have even lower priority in other Finnish maritime schools. In Novia University of Applied Sciences they have an IT course for Microsoft Office but it is only worth 1.5 credits. Even worse, Satakunta University of Applied Sciences has decided to make Microsoft Office part of its 'Learning Skills' course which includes also introduction to school's practices and is only worth one credit.

2.2.2 Insurances

One interesting point is whether insurances cover damage caused by a possible cyberattack. Many insurance policies include a cyberattack Exclusion clause which states:

1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software program, or any electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile (Hellenic Shipping News 2016).

Per these clauses insurance companies are not required to reimburse for damages of a cyberattack. The aim of this chapter was to raise a point and insurances will not be discussed further in this thesis.

2.2.3 Automation

Change is coming and there are already solutions where fuel consumption data is sent to the company's office via the internet. It is already possible to remotely access shipboard automation system. For example, if a ship is equipped with Wärtsilä's Integrated Automation System, Wärtisilä's service personnel can connect to the system via VPN connection and have the same view as the engineer on board. Wärtsilä says that even though it is possible to make corrections remotely, they will then guide the crew to make those corrections instead of making the changes themselves remotely (Wärtsilä 2016).

As discussed in chapter 2.1.5, the bridge of a modern vessel is integrated. This allows to automate navigational processes. For example, it is possible to set the autopilot to follow the route planned on ECDIS. This is rarely used practise on Finnish vessels as it takes control away from the officer of the watch. As the automation system tries to keep the vessel directly on the route line, it wears the rudder more than steering the vessel using autopilot's heading mode.

Another example of automation is a vessel equipped with dynamic position system. In this case the control of vessel's propulsion system is given to computers that execute orders given by officer. This system relies heavily on accurate GPS data to keep vessel in place, making if rather vulnerable to spoofing described in chapter 2.1.4.

2.2.4 Autonomous vessels

Rolls-Royce is currently studying the possibility of having autonomous vessels replacing conventional vessels in the future. Their project AAWA (Advanced Autonomous Waterborne Applications Initiative) is funded by Tekes and they have co-operation with several Finnish universities. They are now studying technological, safety, legal and economic aspects of autonomous shipping. They claim to have a proof of concept by the end of 2017 and to have a remote controlled vessel in commercial use by end of 2020. In their vision, they will have an ocean-going autonomous vessel in 2035 (Rolls-Royce 2016, 2).

Having a completely autonomous vessel requires large amounts of sensor inputs which must be processed by a computer system which understands the rules of the road at sea. In order to have a computer that makes all the navigational decisions while an operator is overseeing multiple vessels from a remote station may seem a little far-fetched now but the rapid development of computer technology may make this possible in the coming decades.

Antti Äijälä lists a few problems on autonomous shipping in his bachelor's thesis 'The Risks of Operating an Autonomous Vessel'. One of these is data transmission. He says that at present there are no means of transmitting large amounts of data rapidly and effectively over vast distances (Äijälä 2015, 26). *Communication will need to be bidirectional, accurate, scalable and supported by multiple systems – creating redundancy and minimising risk* (Rolls-Royce 2016, 3). Even though vessels would be completely autonomous, they will be accessible via the internet making cybersecurity even more important.

Rolls-Royce acknowledges cyber risks and says that it would be possible to remotely take over the control of the vessel in malicious purposes. They also know the possibility of jamming or spoofing AIS or GPS that were handled in chapter 2.1. To minimize the risks Rolls-Royce suggests to eradicate the vulnerabilities of vessel's computer systems and to add intrusion prevention and detection. Systems need to be updated on a regular basis and data needs to be encrypted and verified (Rolls-Royce 2016, 66). All in all, the same things that should be taken into account on conventional vessels. Even the human factor remains as the remote operator still has access to the vessel's systems.

3 CYBERTHREATS

There are various cyberthreats in existence, a few of them are listed here. Many threats rely on the human element, as direct attacks are often blocked by proper use of firewalls and other security measures.

3.1 Social engineering

As it is with every technical device, users are always the weakest link in the security chain. Their actions present a security hole that can never be completely plugged. Secondly, attack from the inside creates the largest threat to overall security. The worst-case scenario is created when an inside attacker is unaware that he is one (Walker 2012, 194).

Social engineering is the art of manipulating a person, or a group of people, into providing information or a service they otherwise would never have given. For example, most people would never give their password if asked directly. However, many would give just that if asked by someone seemingly trustworthy, such as help desk employee or network administrator. Social engineering can be divided into two categories: human-based and computer-based (Walker 2012, 195).

Human-based engineering uses interaction in conversation, email or other means between people in order to gather information. These means usually require physical access to target location which can be obtained by claiming that you forgot your ID badge home and ask an authorized person to let you in. Means to obtain information can be as simple as dumpster diving: going through discarded papers looking for passwords, employees contact info or information about a company's network. One could also pretend to be a valid user, such as tech support person, and convince an employee to grant access to company's computer. The attacker could also contact IT support claiming to be a user in that company and request password reset. An attacker could also look over the user's shoulders, or from a long distance using binoculars, as they log in and therefore gain login credentials. Eavesdropping may also reveal valuable information. One devious method is known as reverse social engineering where the attacker manages the target to contact the attacker. This way the target trusts the attacker more compered to situation where the attacker would contact the target. For example, the attacker sends an email to a group of users warning them about "network issues tomorrow" and has provided a phone number for "help desk" if they are affected. The next day, the attacker performs a simple denial of service attack to target machine and waits for the user to call him. Then he simply asks for the user's ID and password so the attacker could "solve the problem" (Walker 2012, 195-197).

Computer-based attacks are carried out by using a computer or other data-processing device. These include specially crafted pop-up windows, tricking user to click through a fake website and false SMS texts. Social media can be used to gather information to make the false messages to seems more sophisticated and believable (Walker 2012, 198).

3.2 Phishing and Spear phishing

Phishing attack consists of crafting a seemingly legit email which contains links to fake website or to download malicious content. The email may appear to be from a bank, credit card company or other various legitimate business. Should the user click the links, the attacker gains all the information the user inputs to the fake website. These emails can be terribly deceiving and even a seasoned user can be tricked. The best way against phishing emails is to educate users how to recognise them. Here are a few examples of how to recognise fake email:

- Unknown sender. Even if the email is seemingly from someone you know but the content seems to be out of place, it is still something to be cautious about.
- Greeting. It should ring bells if the email is not specifically addressed to you but uses something general such as “Dear member”.
- Phone number. If the email contains a phone number, you should check its validity before calling to it, preferably not at all.
- Spelling and grammar mistakes. Emails from genuine businesses are always written using proper words and grammar.
- Hyperlinks. Check the links before clicking them. Hovering mouse over the link reveals the actual website the link would take you to.

Spear phishing is more advanced and dangerous version of phishing. Here the attacker has collected information about the victim using other means of social engineering. The basic idea is still the same: to send an email containing links to fake websites. However, this time the target is greeted using his or her name. The email contains legit information about the target making the target less suspicious (Palo Alto Networks 2016, 7).

Phishing is not always carried out using emails. Social media has become an important platform for phishing and methods such as a link on Facebook or on a message board or a shortened URL on Twitter are not that rare anymore. These methods allow the attacker to collect information about the target for spear phishing (Palo Alto Networks 2016, 7).

3.3 Watering hole

A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment. Watering hole attacks, which tend to focus on legitimate, popular websites, are a derivative of pivot attacks, which target one thing to get at another. In a watering hole attack, the attacker first profiles its targets -- who are typically employees of large enterprises, human rights groups or government offices -- to determine the type of websites they frequent. The attacker then looks for vulnerabilities in the websites and injects malicious JavaScript or HTML code that redirects the target to a separate site where the malware is hosted. This compromised website is now ready to infect the target with the injected malware upon access. (TechTarget 2015).

While watering hole attacks are uncommon, they pose a considerable threat since they are difficult to detect and typically target high-security organizations through their low-security employees, business partners, connected vendors or an unsecured wireless network. (TechTarget 2015).

3.4 Malware

In the past, malware was only a swarm of independent agents that only infected machines and replicated themselves, making detection rather easy. Modern malware can be difficult to notice, and according to Global Security Report, on average it takes 188 days from infection to detection. This is because malware is able to mutate or it can be updated to avoid detection by

traditional antimalware signatures. Malware can also be crafted specifically against certain individual or organization (Palo Alto Networks 2016, 14).

Malware can also be delivered using a drive-by download. This way the user is unaware while the malware is downloaded by taking advantage of a vulnerability in an operating system, web browser or an application. Using a software exploit the malware can also trick an application, such as web browser, to run its code. Once a computer has been infected, malware ensures its survivability on that machine by various means, such as creating a backdoor, granting root-level access or even by disabling AV software. After that malware is ready to be used by the attacker to take control of the target or to gather information. However, this communication must be stealthy. This can be achieved by encrypting the communication, circulating the traffic or by using port hopping (Palo Alto Networks 2016, 16-18).

Traditional firewalls use ports and protocols to identify and filter traffic. This will be ineffective against malware that hop from port to port until they find an open connection to the network (Palo Alto Networks 2016, 28).
A next-generation firewall performs a true classification of traffic based not simply on port and protocol, but on an ongoing process of application analysis, decryption, decoding, and heuristics. These capabilities progressively peel back the layers of a traffic stream to determine its true identity. The ability to pinpoint and analyze even unknown traffic — without regard to port or encryption — is the defining characteristic of a true next-generation firewall and is invaluable in the fight against advanced malware, exploits, and other sophisticated threats (Palo Alto Networks 2016, 34).

3.5 Denial of Service

Once an endpoint has been infected malware, it becomes a bot which can be part of a larger botnet. These botnets are often used to overwhelm target server or network with enormous amounts of traffic. This is known as distributed denial of service (DDoS). Bots themselves are not the target, and often are unaware of the infection, but they are effective tools to be used (Palo Alto Networks 2016, 9). A few ways to reduce the risk of DoS is to disable

unnecessary services, using a good firewall policy and keeping software and hardware up to date (Walker 2012, 298).

4 SHIPS' NETWORK STRUCTURE AND IT PRACTICES

The primary objective of this thesis was to investigate what sort of networks are installed on board and then evaluate whether there is room for improvement. I was able to study two different ship's networks. It was agreed with the ships' masters that ships, companies and possible third parties remain anonymous and from now on the vessels shall be referred as ship A and ship B.

4.1 Ship A

One could compare a ship's network to a small company's network. There are some small differences, such as the absence of a fixed the internet connection due to ships' mobile nature. Ship A's network structure can be seen in Figure 2.

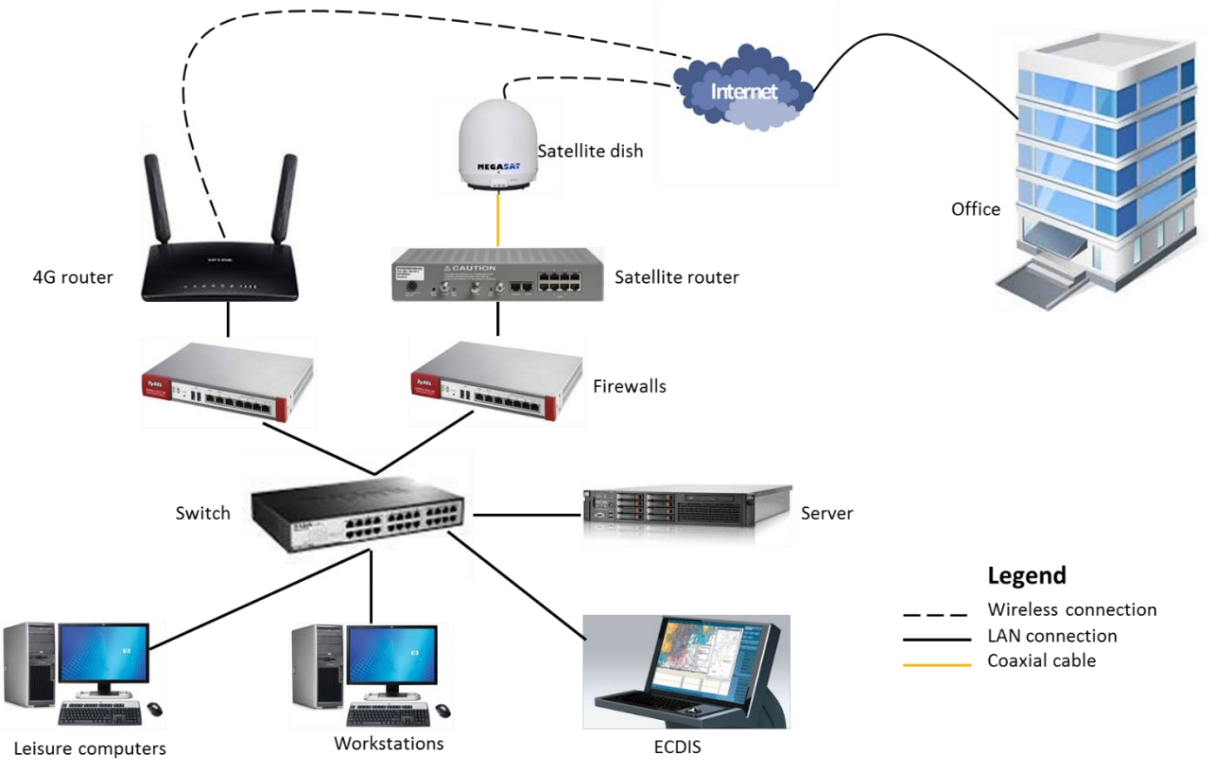


Figure 2. Network structure of Ship A

The internet was provided via either 4G network or satellite connection. On this vessel, 4G connection was used only near Finland's shoreline, as the use abroad would be expensive due to the amount of data. Therefore, the satellite connection is used primarily. Both the internet connections go through the ship's firewalls to prevent unauthorized access.

The nexus of ship A's network is a switch which connects all the devices together. However, the ship's network is part of the whole shipping company's network. For example, the email server and some of the databases are physically located in the office ashore. The ship's computers are connected through a VPN connection to the office.

The server on board handles active directory, DHCP and backups. DHCP is configured in such way that only ship's own computers static IP addresses are allowed. Even if one would plug in your own computer to the network, the server would not give access. The network is also configured to prioritize based on computer and traffic type. For example, the email traffic of master's computer has one of the highest priorities while a leisure computer's access to a news site is far down in the priority configuration.

Backups are taken daily from crucial systems and saved in the server. In addition, senior officers have external hard drives for taking their own backups.

All the computers on board had AV software installed on them. They also had remote connection software so that company's own IT department can make connection if need be.

One interesting fact was that the leisure computers are also connected to the company's domain. It is understandable when considering how the network is designed to work. Access to some web sites is denied, for example adult entertainment sites.

On ship A, the ECDIS is provided by Furuno. Their solution for updating ECDIS is to connect it to their own servers which can be seen in Figure 3. When UKHO publishes new chart updates, Furuno's servers download them and send the files via satellite connection to ship's Gate-1 unit. From there the

navigation officer installs updates to ECDIS. What is worrying is that ECDIS is connected to Gate-1 via Ethernet cable. Furuno says that the connection is authenticated by RSA keys and encrypted by AES (Furuno). Despite these security measures the fact that there is direct connection between ECDIS and the internet remains. This is particularly dangerous as ECDIS has no AV software and it is running on Windows XP.

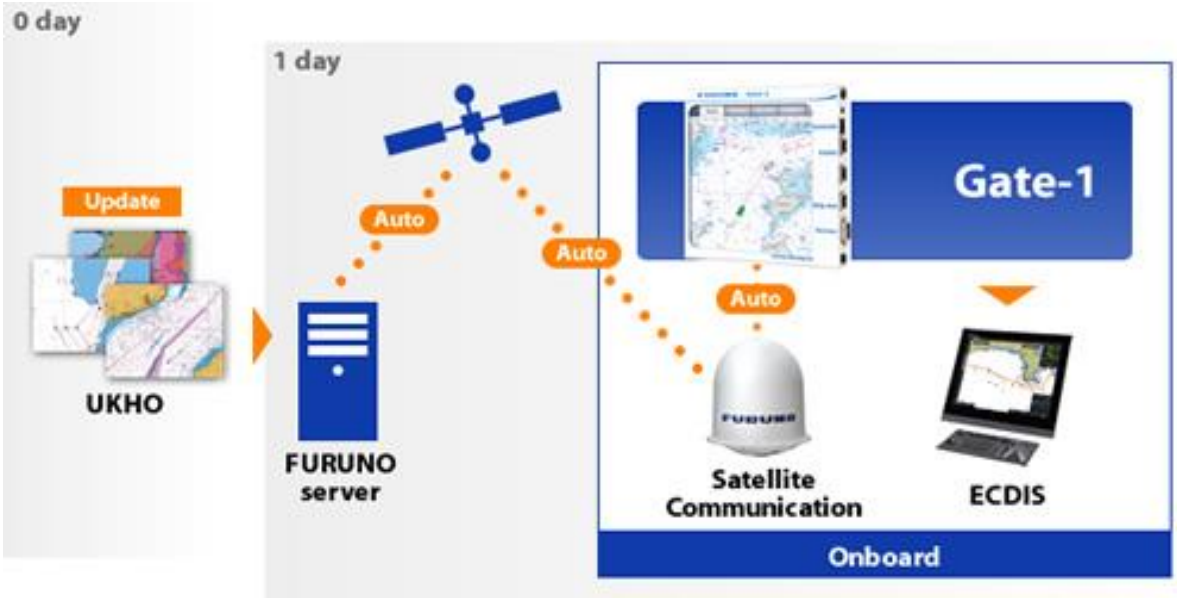


Figure 3. Furuno's ECDIS chart update system (Furuno http://www.furuno.com/en/merchant/ecdis/gate-1/)

There were some general instructions and guidelines for cybersecurity in ship A's Safety Management System. There were no dos and do nots. This was peculiar as some tasks are described in great detail in the SMS.

4.2 Ship B

As can be seen from Figure 4, the network structure of ship B is rather similar with ship A with some minor differences.

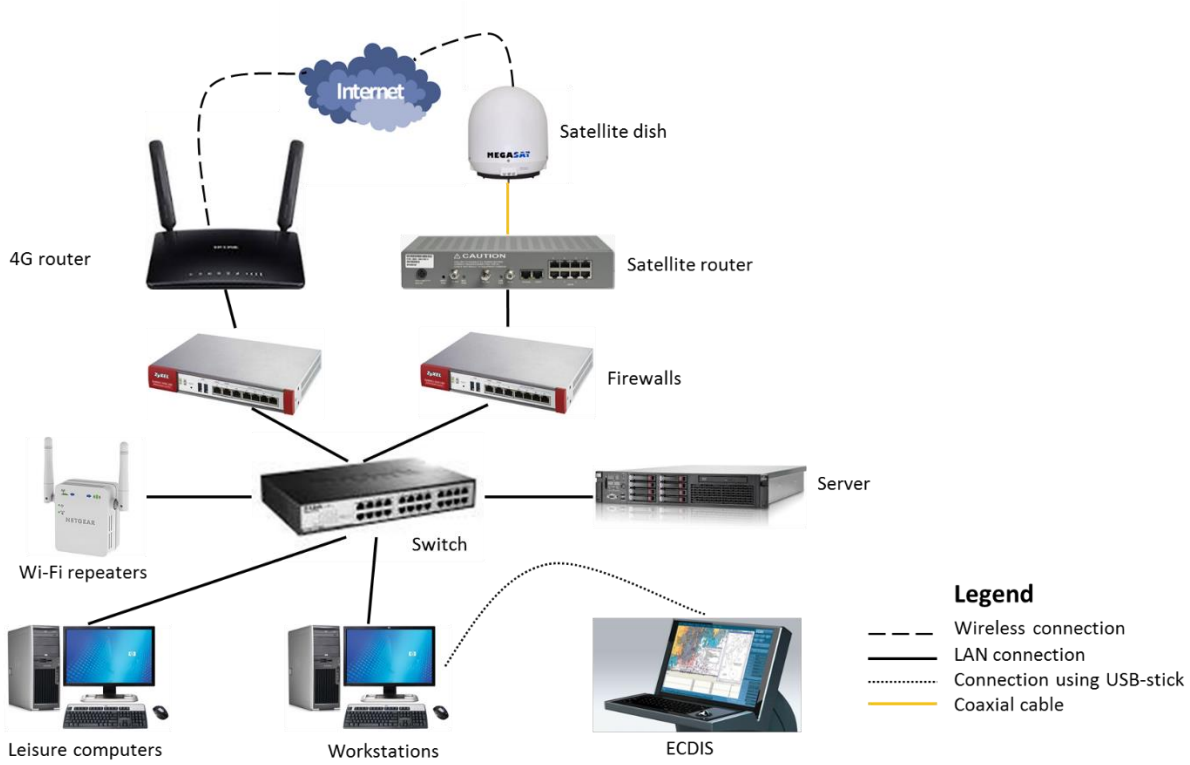


Figure 4. Network structure of Ship B

The internet is accessed in the same way as in Ship A. However, on this vessel 4G connection was allowed abroad. Nowadays almost all ships are equipped with satellite connection as exchanging emails has become crucial part of shipping industry. That is where similarities end.

Ship B is an independent unit and it is not connected to shipping company's network. All the services are installed in the onboard server. In this case, each of the shipping company's vessels had their own domain as the previous case each ship was part of the company's domain.

The switch is configured to have two VLANs: one for the ship's own computers and the other for crew's personal computers. The ship has workstations and leisure computers connected to the switch via Ethernet cable. They seemed to be in good condition as they were running Windows 7

and they had AV software installed. Then I discovered a laptop in the crew's coffee room which was running Windows XP and had no AV software, therefore compromising the whole network.

The IT support is outsourced to a third party which administers devices, network and provides support. Onboard computers had a remote-control software installed on them.

The other VLAN was meant for the crew's personal use. There were Wi-Fi repeaters on each deck. Due to the vessel's solid structure, the repeaters have a limited range, and it is not possible to access the network from shore even when the ship is at berth. The network was protected with a WPA key but there was a problem: the password was written to each repeater, allowing possible unauthorized access. There was also another problem as the administrator passwords for the routers were written on a paper in the bridge. The saving grace is that unauthorized physical access to ship is rather difficult due to arranged security measures per the ISPS. The administrator passwords for the server and the switch were only known by the third party.

Keeping ECDIS up to date was arranged in a different way than in ship A. In this case, ECDIS had no the internet connection. Updates were downloaded with bridge workstation and then transferred into a dedicated USB stick, which was then plugged to ECDIS. It was said in the company's SMS that the stick must be scanned for viruses each time it is plugged in. Here ECDIS ran also on top of Windows XP, making it vulnerable to infections via the USB stick as there is no AV software installed.

4.3 Attack scenario

Let us think about a scenario how to take advantage of ship A's network. The attacker starts by looking possible victims from LinkedIn. He finds Oscar Officer, a recent graduate from maritime school working as a junior officer onboard ship A. The attacker gathers information about Oscar from social media. Then a spear phishing email is crafted specifically targeted for Oscar.

Few days later Oscar opens up his personal email account on the vessel's computer and notices that he has been approached by a renowned cruise

ship company. He is greeted by name, complimented on his achievements and offered a position on their new vessel. All Oscar has to do is to simply fill in the attached contact form and send it back to them. Having delusions of grandeur about himself, Oscar has no second thoughts and opens the attached PDF file. Unknown to him, the PDF has hidden piece of malware included that runs when the file is opened. The attacker has now access to this computer.

The next step for attacker is the identify what sort of network he is facing. As he is aware that networks onboard vessels are not as secure as they should be and that it is unlikely that there is no IT person onboard, he starts to scan for open ports, operating systems and running applications. Now he may also start to listen the traffic for information, such as user accounts and passwords, using man-in-the-middle attack. At some point, he finds out that there is an ECDIS software running on top of Windows XP. He uses vulnerabilities of the operating system to access the computer. He then decides to have some “fun” and changes the location of few crucial navigation buoys as described in chapter 2.1.2.

5 HUMAN FACTOR

Despite all the advanced systems and devices we have, there is always a human operating them. This will eventually lead to a human error which can have severe consequences. *Cybersecurity just as much a question of culture and attitude as it is technology. The best encryption algorithms in the world are useless if someone writes the password on a Post-it note and leaves the door open* (Hansen & Rahman 2013, 1). Training the officers to use these tools efficiently and safely is the key for avoiding accidents.

The second objective of this thesis is to study the competence of Finnish officers regarding their IT skills and the internet security awareness. I conducted a survey where each officer filled in an Excel sheet in my laptop containing 26 questions. The survey was conducted as structured interview as I had fixed question form (Hirsjärvi, Remes & Sajavaara 2008, 203). The survey can be found in Appendix 1. There were a total of 17 answers, nine from deck officers and eight from engine officers. The ages of the officers

varied between twenty and sixty years. This survey is not scientifically accurate but more of a directional sort as the number of answers is rather low.

In hindsight, it would have been a good idea to have an external mouse since some people struggled using the laptop's integrated mouse. Some questions could have used more refinement since some of the officers found them a little confusing and they had to ask what I meant with the question in hand.

I tried to find some existing surveys which I could use as a base for my own survey but to my surprise I was unable to find one. There were a few that were somewhat near of what I wanted but not close enough to be used for this purpose. Therefore, I created the survey from scratch. I designed the questions to be simple and close to earth since my assumption was that officers do not have deep knowledge about computer technology.

The purpose of this survey is to find out:

1. How officers feel about their own IT skills?
2. What kind of experience they have with computers?
3. How aware they are about cybersecurity risks?

5.1 Backgrounds

The first six questions asked about officers' backgrounds with computers and information technology in general. The survey began with a question asking officers to evaluate their own IT skills. This can be seen in Figure 5.

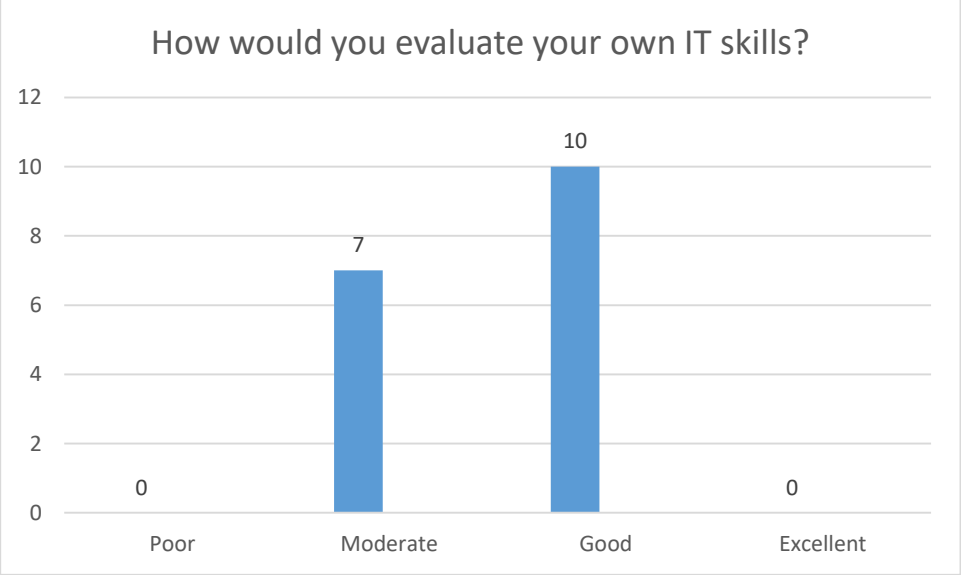


Figure 5. Results of IT skills evaluation

The results are twofold. It is good to notice that none of the officers considered their skills as poor. On the other hand, it is worrying that there is no one who feels their skills as excellent, especially as computer related duties are becoming more and more solid part of officers' daily routines.

Next the officers were asked if they have a degree in IT related subject and if they have been on IT courses. Results are as shown in Figure 6.

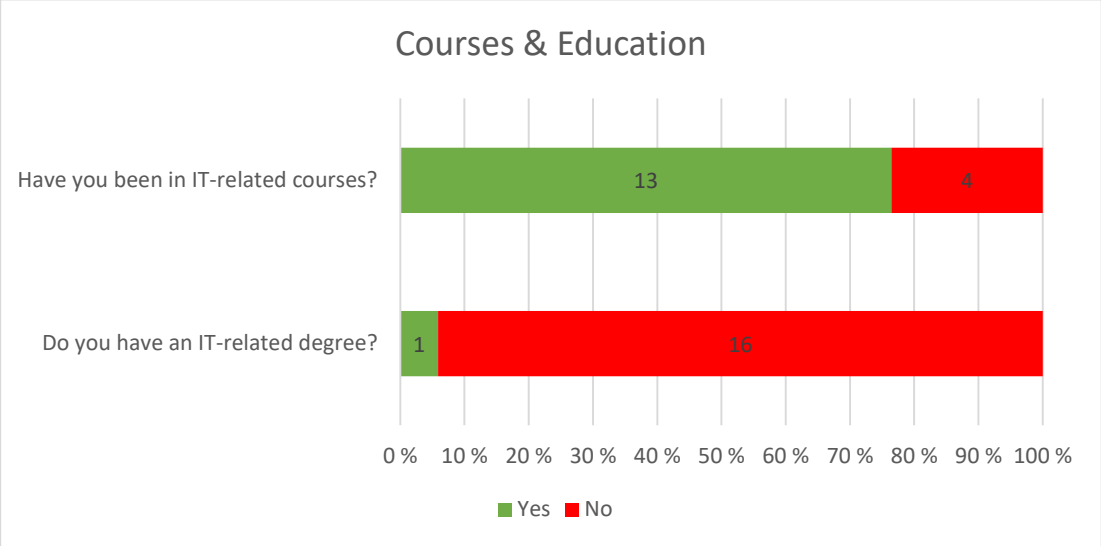


Figure 6. Results of courses & education

The person who answered to have a degree, specified later that he had started to study computer science in a university but dropped out during his first year of studies. The rest had no previous education on IT. It was comforting to find out that the majority of officers had taken some courses. On next question, they were asked to specify what courses they had taken and it was allowed to mention multiple courses. The results can be seen in Figure 7.

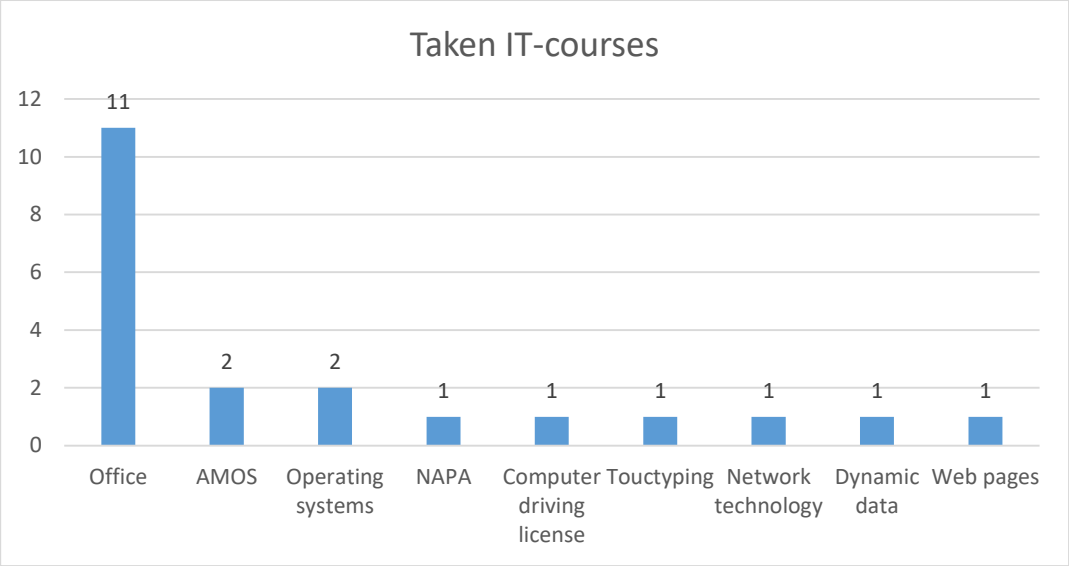


Figure 7. List of taken IT courses

The majority of the officers had taken some course regarding Microsoft Office, but some said that they counted the course provided by school during their maritime studies. The rest of the answers were divided. Two persons had taken a course about using Windows based operating system efficiently. It is a good choice since it makes their everyday life easier. Also, two persons had taken a course on AMOS. I have briefly used AMOS and I found it highly confusing as it seems a rather complex program but after taking an introduction course for AMOS everything became much easier to understand. Since using AMOS is a daily routine for engine officers and rather usual for deck officers, it would have been logical to assume that more people would have taken course on it. The rest of the answers are more difficult to analyse but they are interesting as there are also some advanced subjects as network technology and dynamic data. These are not essential in onboard duties but more on nice to know basis.

When asked if they felt like they needed more training on some subject, seven persons answered yes. They were then asked to specify what subject they wished to learn better. It was allowed to give multiple answers. The results can be seen in Figure 8.

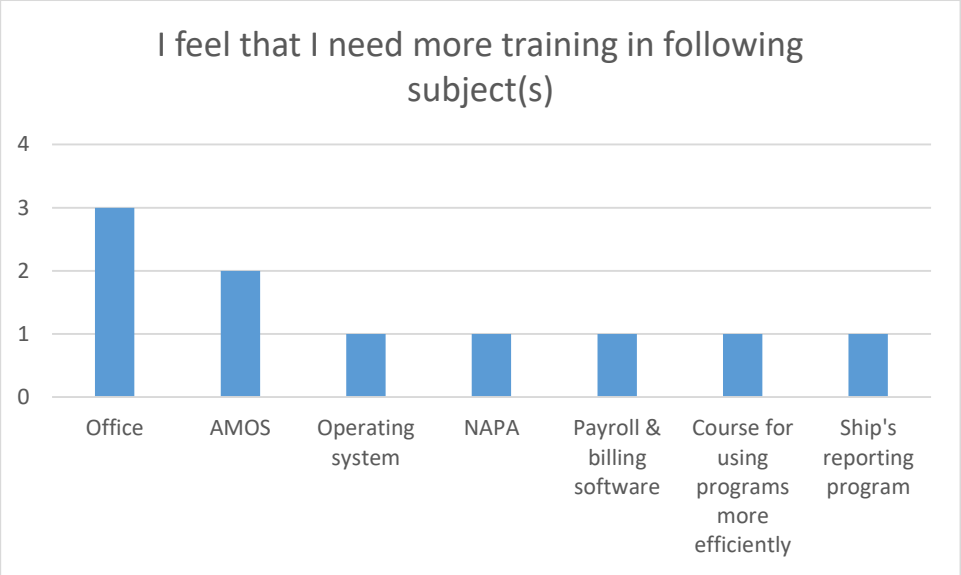


Figure 8. Results of I feel that I need more training in following subject(s)

Microsoft Office was the most popular answer. It is good to find that the officers recognize themselves if they need more training as Microsoft Office programs are part of their daily routines. The same goes for AMOS. The rest of the answers are more distinct. One of the officers felt that he is not comfortable with recently installed Windows 10. One navigation officer answered that he needed training in new programs used to send the ship's traffic information to the Finnish Transport Agency.

5.2 IT skills

In this chapter, we delve into officers' IT skills. First, it was found out how they handle situations when they encounter computer related problem. Most of the officers would contact IT support when faced with a problem as can be seen in Figure 9.

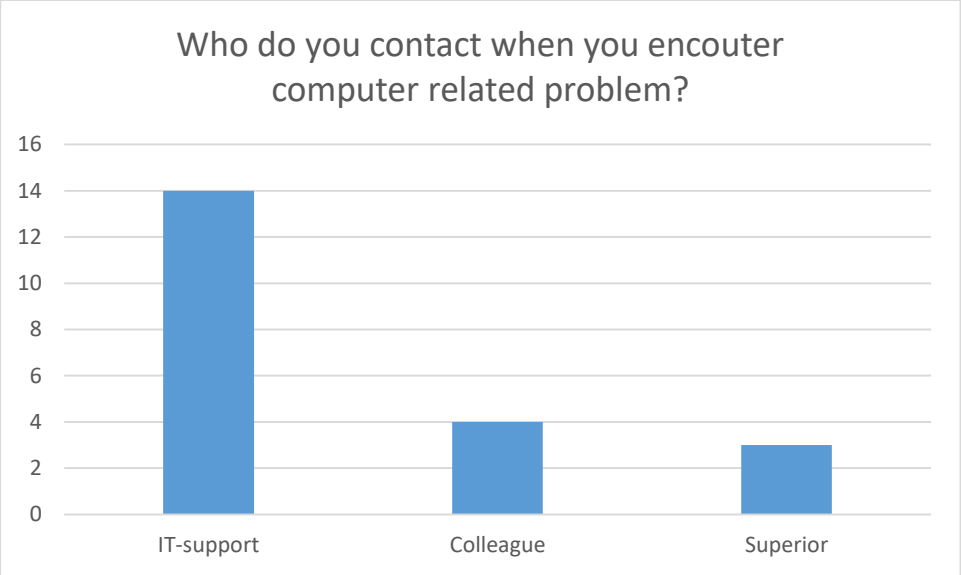


Figure 9. Results of who to contact in case of computer problems

The officers were allowed to answer freely, so some answered that first they would ask their colleague or superior and then would contact IT support. This is a good practice since it will not trouble the support unnecessarily as there is a chance that answer can be found just by asking someone else. There is also possibility that the vessel is at open sea so the internet connection is very limited making remote access challenging. The rest of the questions concerning officers' IT skills can be seen in Figure 10.

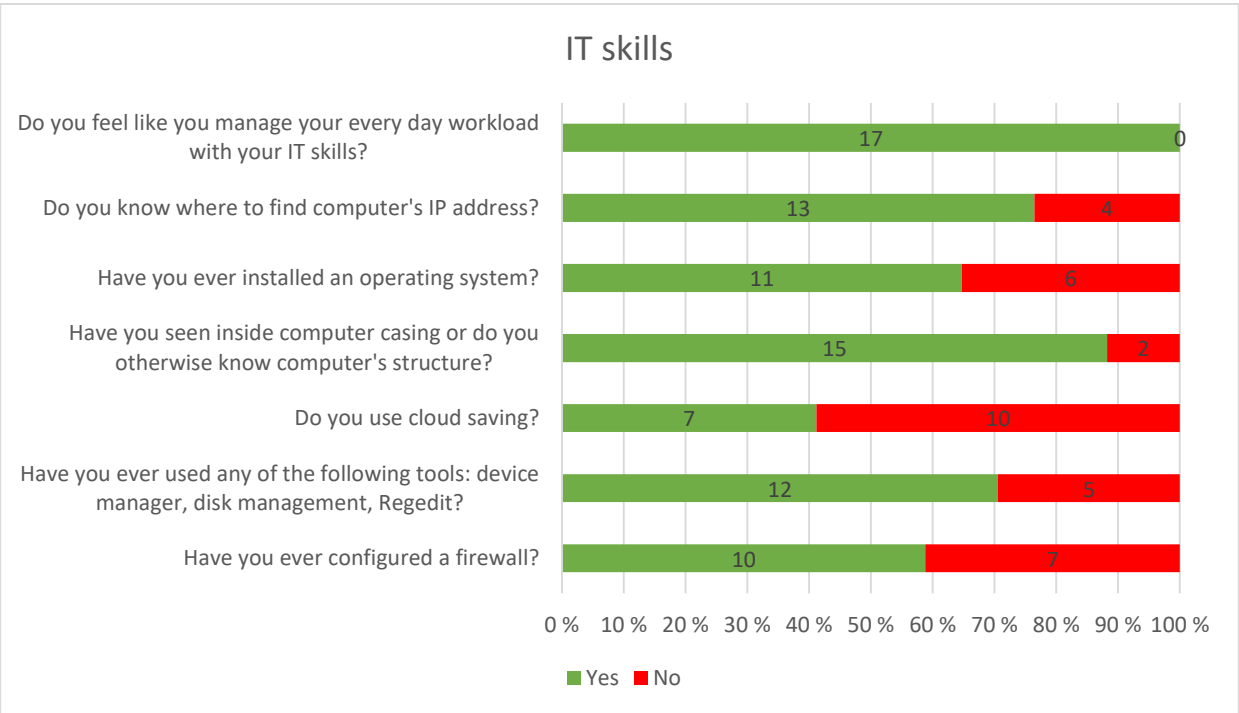


Figure 10. Results of IT skills questions

It is great to see that everyone thought they can manage their computer related duties. In their own mind, their background training and onboard familiarization are enough to cope with their tasks.

Majority of the officers knew where to look computer's IP address. This is a good skill to know when solving the internet problems. Sometimes it is enough to reset IP address and other times IT support may ask the user to tell them the IP address.

Although it is not necessary to know how to install an operating system, it is good to know what happens during installation. This can be counted amongst nice to know skills to make everyday duties a little easier as you have some basic understanding what is happening in the background. Keeping this in mind, it was good to find out that two thirds of the officers had installed an operating system.

Almost everyone knew from what components computer consists of. However, this is not essential information as it is rather rare that one should open a computer and change a component. Usually, when a computer breaks down, IT support comes to replace it with a new unit so even they will not replace single components.

It was rather disappointing to find out that less than half of the officers used cloud saving on their personal files. As it is quite easy way to make backups of one's files and to ensure that they are available when one is on the road, it would be desirable that more people would use cloud saving.

It was positively surprising when twelve officers answered having used Windows' advanced tools. Those are great help when solving problems concerning external devices and other problems. Regedit is the rarest of these tools and some officers did not know what it is.

The number of officers that had configured a firewall was also positively surprising. When they were asked to specify what they had done, they answered that they had opened ports for programs. Therefore, it would be safe to presume that they have been dealing with either Windows' or router's firewall settings but in my opinion this is good enough.

5.3 Security awareness

Security awareness is the most important part of this survey. Here it is found out whether the officers know to avoid cyber threats in their everyday practices. The results can be seen in Figure 11.

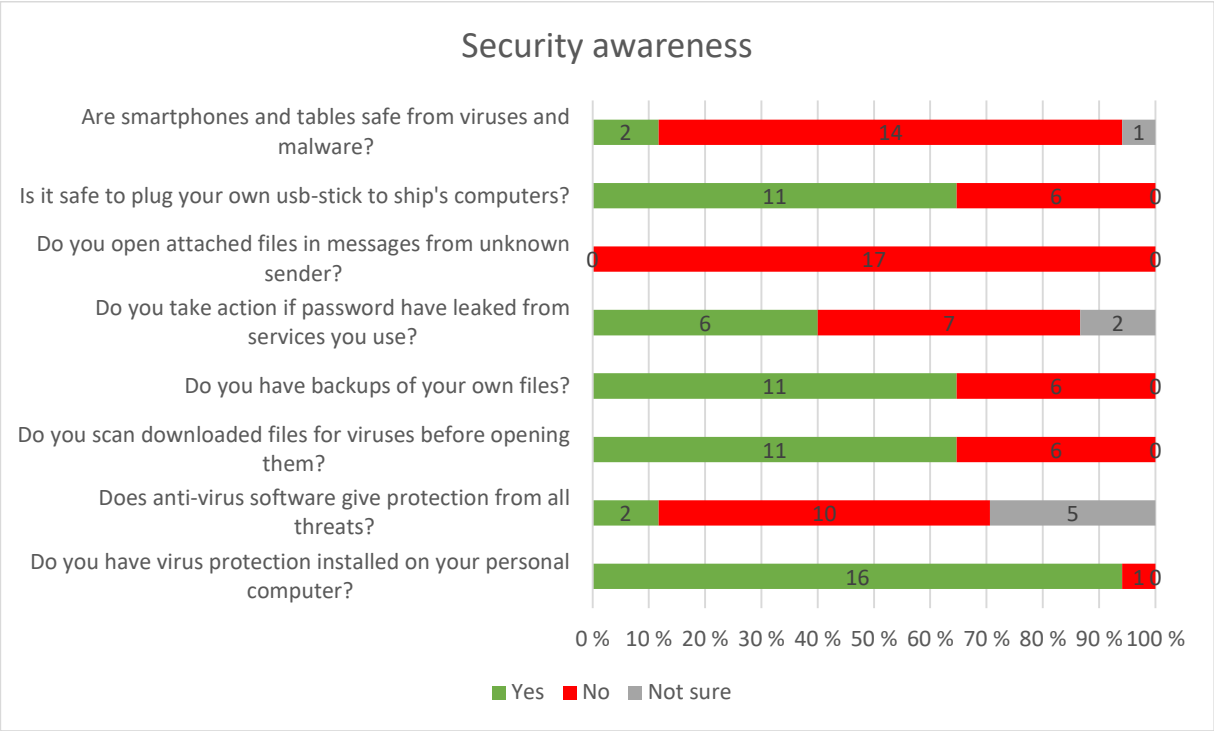


Figure 11. Results of security awareness questions

Most of the officers were aware that smartphones and tablets are vulnerable to threats. This is good since there might rise a need to plug your phone or tablet to ship's computer to transfer files. This, for example, is one of the most probable ways to infect ship's computer, therefore they should be aware of that.

The same goes for plugging your personal USB stick to the ship's computers. It is quite worrisome to see that over half of the officers thought that it is fine to plug in one's USB stick. Some of them claimed that it is acceptable because the computer's antivirus software scans the stick each time it is plugged in. *No effective defenses from USB attacks are known. Malware scanners cannot access the firmware running on USB devices. Behavioral detection is difficult since behavior of an infected device may look as though a user has simply plugged in a new device. Blocking or allowing specific USB device classes and device IDs is possible, however generic lists can easily be bypassed. Pre-*

boot attacks may be prevented by use of a BIOS password and booting only to the hard drive (Security Research Labs 2014). Keeping that in mind one should be always aware what they are doing when plugging in a USB device.

It is good to see that no one would open files sent by an unknown sender. This is one of the most probable ways to infect computer as it is used on many types of attacks such as phishing.

Two thirds of the officers had backups of their own files. Although this is not actually an IT skill, it gives an overview of that person's skills and attitudes.

Also, two thirds of the officers said that they scan downloaded files for viruses before opening them. Although this is not necessary if one is sure that the file does not contain any malicious software, it is always better to be safe than sorry.

When asked if antivirus software gave protection from all threats, the results were not that good. Two persons claimed that it would protect from everything and five persons were not sure. Everyone should be aware that there is always a way around antivirus software.

All but one had antivirus software installed on their computer. Some even added that they had antivirus software also on their tablets and smart phones. The one person who did not have AV software said that he had a Mac and claimed that Macs do not get viruses. This might have been true some years ago, but the situation has changed. Bogdan Botezatu, a Senior E-Threat Analyst from Bitdefender, says Macs can definitely be infected by viruses. *Mac OS X software has more high-risk vulnerabilities than all versions of Windows put together. Apple markets these products as virus-free. They say you do not need an antivirus, because they know people hate antivirus software. These utilities often slow down your computer, so they do not want to promote them* (Hill 2015).

It was good to see that everyone had at least two passwords as can be seen in Figure 12.

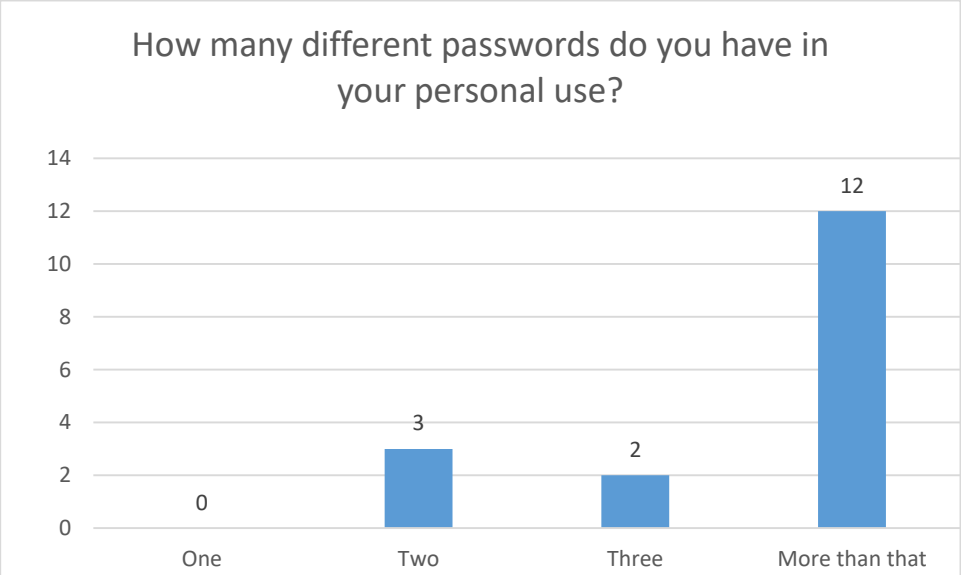


Figure 12. Results of number of passwords

Even better, most of the officers said that they have more than three different passwords in use. It is important to have multiple passwords, as if one of them is compromised then not all the services one uses are threatened.

To find out how strong the officers passwords are they were asked how many different attributes their passwords had as can be seen in Figure 13.

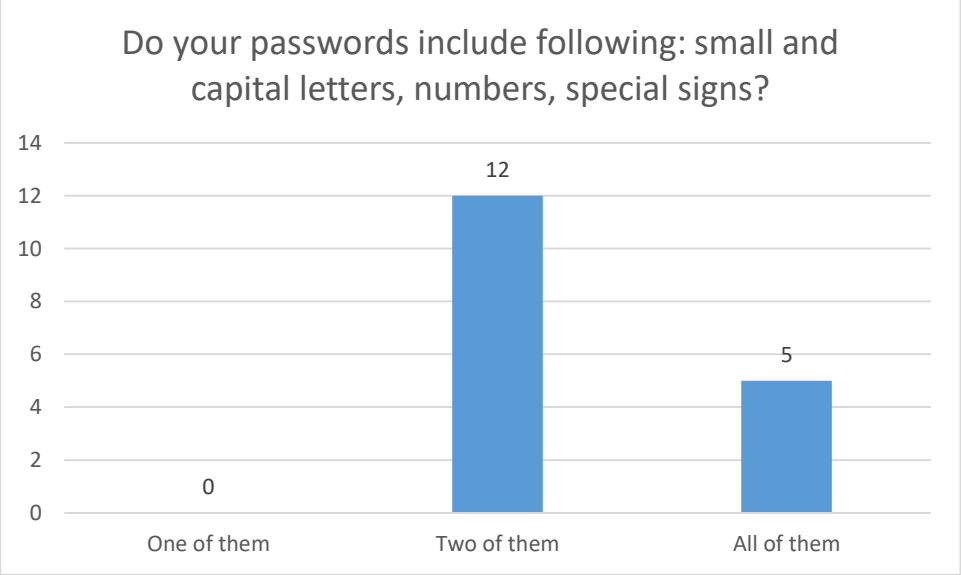


Figure 13. Results of quality of passwords

Most of the officers said that their passwords included two attributes. If one had to speculate, it would seem that these would be small and capital letters and numbers. The complexity of password is important but the length of the password is even more important as it makes the amount of possibilities to grow exponentially. The randomness of the password is also an important factor. It is much easier to guess the password if it consists of dictionary words.

The result of virus scan frequency was rather divided, as can be seen in Figure 14.

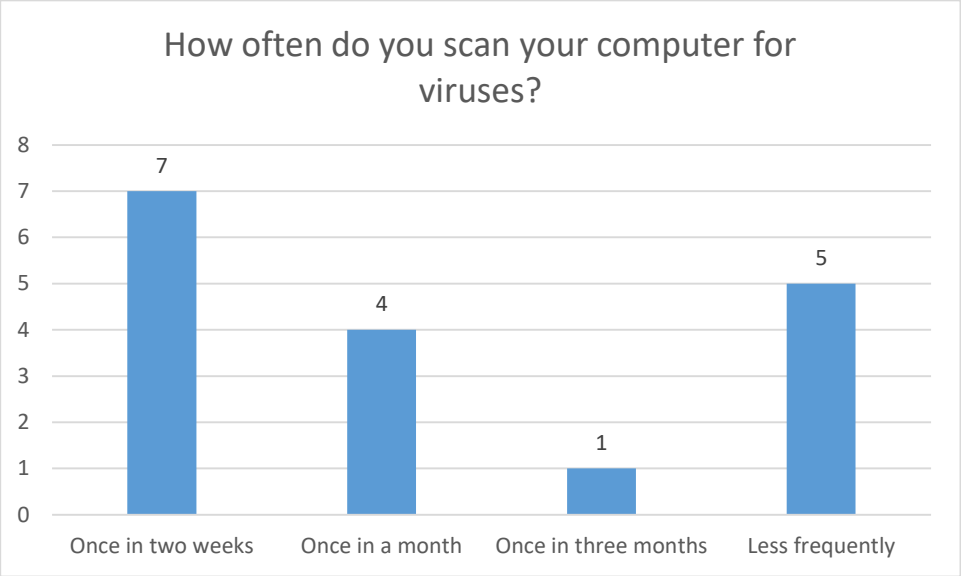


Figure 14. Results of frequency of virus scans

Seven said that they scan at least once in two weeks. Some added that their AV software is set to scan automatically every week. This is a good thing as it reveals possible infection quite early and does not require any actions from the user. On the other hand, it was terribly disappointing as five answered that they do not scan their computer even once in three months. This makes possible infection even worse as it will not be discovered for a long time.

To summarize this survey, the results were better than initially expected. However, there is still room for improvement. Even though everyone said that they can cope with their daily duties, there are things that they should be more aware.

It is not realistic to expect every vessel to have access to IT and cybersecurity expertise; however, most people today have some level of IT knowledge and security awareness through using their private computers (Hansen &Rahman 2013, 4). This will be addressed more profoundly in the next chapter.

6 CONCLUSIONS & RECOMMENDATIONS

6.1 Network

Firstly, it must be admitted that the descriptions of the studied vessels' networks are incomplete as I was unable to study how switches and firewalls are configured. This would be crucial information in determining the complete integrity and security of the network. However, some conclusions can be drawn from what is known.

As both shipping companies had proper IT departments, it is rather safe to assume that firewalls and switches are configured properly, both ship A and B have secure networks. However, even in this case network A is more vulnerable as computers are not separated in any way. The weak point is the leisure computers. As crew members use these computers for their personal affairs there is always a risk for infecting the whole network. With this in mind, network B is more secure as it allows crew members to use their own computers through a separate VLAN and therefore keeping them apart from vessel's computers.

This subject should be studied further. It was agreed with my supervisor that the best course of action would be to offer a shipping company an evaluation of their network. In this way, it would be possible to gain a complete access to the network and devices. The evaluation should be done in co-operation between an IT and a marine student. Co-operation between two students would be essential in order to get proper understanding of the network and its vulnerabilities and what could be caused to navigation and other systems. The shipping company would also benefit from this arrangement as they would gain valuable information (Kettunen 2017).

Even though the studied networks can be considered secure there is always room for improvement. One solution could be to use a firewall to zone devices from each other with different purposes. An example can be seen in Figure 15.

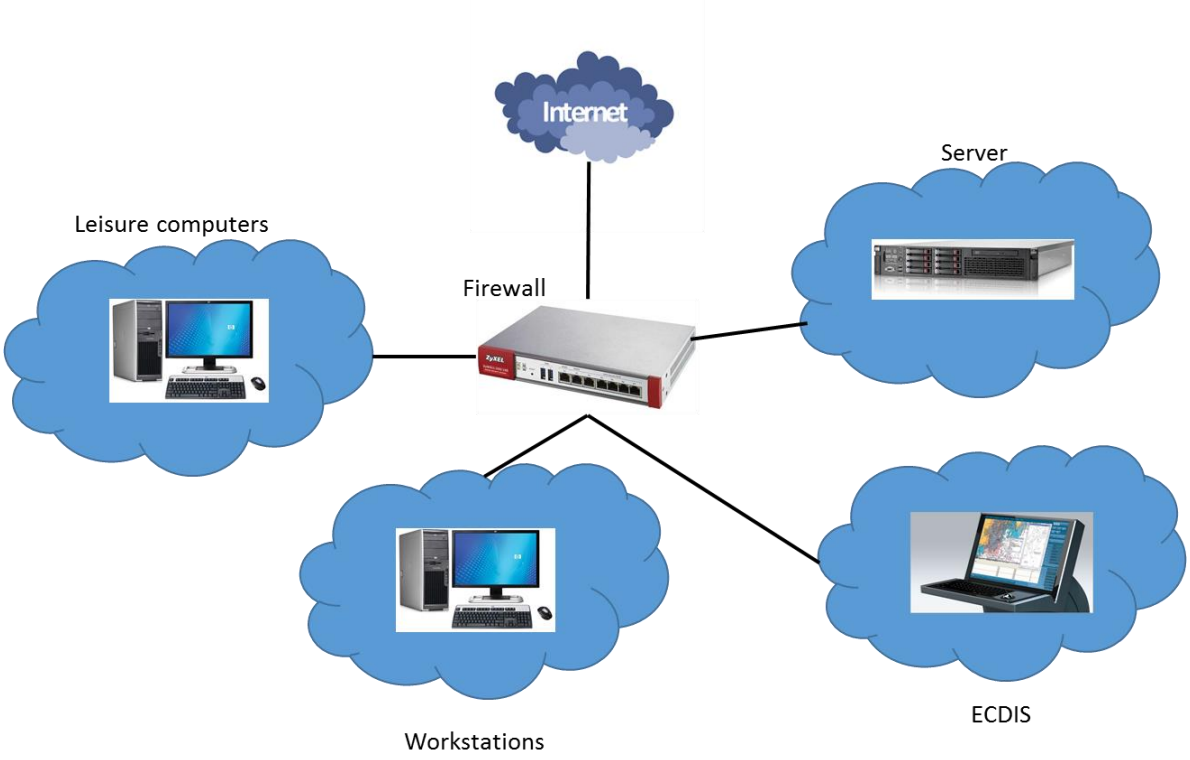


Figure 15 Improved network

In this case the logical nexus of the network would be a next-generation firewall. The clouds in the figure present different zones. This allows administrators to set up policies for different zones that are: leisure computers, workstations, server and ECDIS. This way it is possible to deny all access from leisure zone to all other zones. In case some computer in leisure zone gets infected it will not be able to spread to other zones (Kettunen 2017).

ECDIS would be allowed to connect to manufacturer's server to download updates but all other traffic would be denied. This way both remote side and client side threats are minimized. I am personally against connecting ECDIS to the internet as I feel threats are greater than benefits. This is because the only explicit benefit from connecting ECDIS to the internet is to make updating easier. However, this will increase the possibility of infection far greater. If ECDIS is connected to the internet it should at least have an AV software and possibly even software based firewall installed. I know this would increase the

costs as one would have to buy the software and ECDIS should have better hardware than mentioned back in Table 1 but as even the most basic ECDIS will cost over ten thousand euros the cost increase would be meaningless in the long run.

Workstations and server would be able to communicate between each other. However, both zones would be allowed to use applications that are essential for working. A possible VPN connection to company's office would be possible in this network.

6.2 Training

Even though the results of the survey were better than my initial expectations, there is still a lot of room for improvement. The worst part was the number of officers who though that plugging one's own USB stick the vessel's systems is acceptable. This is one of the most probable ways of infecting systems.

The number of different passwords and their complexity was also promising. Passwords that are easy to guess can also compromise even the most protected system. It was good to see that none had passwords that only contained small letters so there is some level of complexity involved. However, it was not one or two cases where the password for some account was written on a paper that was there for everyone to read. Even though gaining physical access to a ship is difficult, it is not a good practice to keep passwords at a visible location.

Overall, officers' IT skills seemed to be in good order when taking into consideration that they do not get that much training for IT. Some officers had even taken some advanced courses on their own and others had learned to use Windows tools by themselves.

There is no cybersecurity related subject taught at Finnish maritime schools nor the shipping companies seem to organize cybersecurity courses for their personnel. Therefore, seafarer's cybersecurity awareness comes from his or her personal interest and experience. This has to change. It would not take too much resources for schools to arrange an eight-hour awareness course. For example, the contents of the course could be the following:

- *Risks related to emails and how to behave in a safe manner. Examples are phishing attacks where the user clicks on a link to a malicious site;*

- *Risks related to the internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;*

- *Risks related to the use of own devices. These devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected;*

- *Risks related to installing and maintaining software on company hardware, where the infection can be propagated, starting from infected hardware (removable media) or software (infected package);*

- *Risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed;*

- *Safeguarding user information, passwords and digital certificates;*

- *Cyber risks in relation to the physical presence of non-company personnel, eg, where third-party technicians are left to work on equipment without supervision;*

- *Detecting suspicious activity and how to report if a possible cyber incident is in progress. Examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network;*

- *Awareness of the consequences or impact of cyber incidents to the safety and operations of the ship;*

- *Understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incidence-response planning and testing; and*

- *Procedures for protecting against service providers' removable media before they are allowed to be connected to the ship's systems.*

In addition, seafarers need to be made aware that the presence of anti-malware software does not remove the requirement for robust security procedures, for example controlling the use of all removable media (BIMCO 2016, 15).

These are basic topics that could be used to make sure that each seafarer's daily actions are secure. Graduated seafarers should undergo a similar training.

I think cybersecurity training should be a made a certificate course but not a certificate of proficiency. Technology and especially security aspects develop and change rapidly so in order to have up to date knowledge the course should be renewed every five years as it is with many other maritime courses.

I hope that some sort of mention of cybersecurity training makes its way to the next edition of STCW. There are many reports and studies, some of which are mentioned in this thesis, that state the importance of cybersecurity awareness for seafarers. There are some vague guidelines but concrete actions are missing.

6.3 IT Officer

No crew member was responsible for onboard IT systems on the studied vessels. This has been the same on other vessels I have been on. It has always been the responsibility of the IT department whether it is company's own or a third-party department. This sort of arrangement is fine if the vessel has short voyages and the the internet connection is reliable. This seems to be the case with many Finnish flagged vessels as they rarely journey beyond the Baltic Sea and the North Sea. But even in this kind of scenario it is devastating if some crucial system would crash and couldn't be fixed as there is no person on board capable of repairing the system.

The concept of having an IT responsible officer, whether from deck or engine department, is an interesting one as there is no such person on merchant vessels. The only one who comes to close to this is the electro-technical officer. However, they are only required to have understanding of the vessel's computer network, not proficiency to work on it. Electro-technical rating has no requirements regarding computer networks (STCW 2011, 172). It would solve several challenges and would lighten the reliability from the IT department. However, there are few problems with this concept. As many vessels are sailing with skeleton crew, officers have their hands full with their current duties. In my opinion, having an IT officer would require vessel to have at least

three officers, excluding the chief officer. Adding a role as significant as this would overload the responsible officer otherwise. IT officer would require extensive amount of training in order to cope with IT duties. They would need to have knowledge of computers and network devices and how to diagnose errors and to fix them.

Lloyd's register has something like this in their mind as they say the following in their guide: The *jobs of seafarers and shore staff need to be re-designed to take account of new or changed responsibilities, including support and maintenance of software-intensive systems* (Lloyd's Register 2016, 5). My interpretation is that this does not directly point to creating an IT officer but to modify current duties of officers.

The following is purely my own concept of a Deck IT Officer:

- The officer would be educated according to STCW A-II/1.
- In addition, they would take IT courses worth of 30 credits including subjects such as computer technology, network technology and cybersecurity.
- Onboard a vessel, they would work as a watchkeeping officer
- They would be responsible for keeping the vessel's IT systems up to date and diagnose faulty devices and try to repair them. They would do this in co-operation with the IT department if possible.
- In order to keep responsibilities clear, they would not be responsible for keeping ECDIS as a software up to date, this would still be the navigation officer's duty.
- They would be responsible for the radio equipment.
- In addition, they would have less frequent duties such as keeping cybersecurity training for the crew, assisting security officer with cybersecurity aspects, planning IT operations with the IT department.

REFERENCES

Balduzzi M., Wilhoit K. & Pasta A. 2014. A Security Evaluation of AIS.

BIMCO. 2016. The Guidelines on Cybersecurity onboard Ships.

Bridge Procedures Guide. 2016. London: International Chamber of Shipping.

Furuno. Automatic Chart Update System “Gate-1”. Available: http://www.furuno.com/en/merchant/ecdis/gate-1/ [Accessed 27 November 2016].

Hansen K.& Rahman A. 2013. Cyber threat to ships – real but manageable.

Hellenic Shipping News. 2016. Cyber Risks and Insurance in the Marine Industry. Available: http://www.hellenicshippingnews.com/cyber-risks-and-insurance-in-the-marine-industry/ [Accessed: 9 December 2016].

Hill, S. 2015. Can Macs get viruses and malware? We ask an expert. Available: http://www.digitaltrends.com/computing/can-macs-get-viruses/ [Accessed: 27 November 2016].

HiMarine Oy. 2016. Introduction to Operation and Maintenance of Bridge Navigation Equipment.

Hirsjärvi S., Remes P. & Sajavaara P. 2008. Tutki ja kirjoita. Helsinki: Tammi.

International Maritime Organization. 1998. MSC/Circ.891: Guidelines for the On-board Use and Application of Computers.

International Maritime Organization. 2016. MSC.1/Circ.1526: Interim Guidelines on Maritime Cyber Risk Management.

Kettunen, M. 2017. Principal Lecturer. Interview 20 January 2017. Kotka: South-Eastern Finland University of Applied Sciences.

Lloyd’s Register. 2016. Cyber-enabled ships.

NCC Group. 2014. Preparing for Cyber Battleships – Electronic Chart Display and Information System Security.

Palo Alto Networks. 2016. Cybersecurity for dummies. 2nd edition. Hoboken: John Wiley & Sons, Inc.

Panda Security. 2015. Operation “Oil Tanker” The Phantom Menace.

Psiaki M. & Humphreys T. 2016. Protecting GPS From Spoofers Is Critical to the Future of Navigation. Available: http://www.spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation/ [Accessed: 9 December 2016].

Rains T. 2013. The Risk of Running Windows XP After Support Ends April 2014. Available: https://blogs.microsoft.com/microsoftsecure/2013/08/15/the-risk-of-running-windows-xp-after-support-ends-april-2014/ [Accessed: 1 December 2016].

Rolls-Royce plc. 2016. Autonomous Ships the Next Steps.

Rolls-Royce plc. 2016. Remote and Autonomous Ships the Next Steps.

Security Research Labs. 2014. USB peripherals can turn against their users. Available: https://srlabs.de/bites/usb-peripherals-turn/ [Accessed: 27 November 2016].

STCW Code. 2011. London: International Maritime Organization.

TechTarget. 2015. Watering hole attack. Available: http://searchsecurity.techtarget.com/definition/watering-hole-attack [Accessed: 28 January 2017].

Walker, M. 2012. Certified Ethical Hacker, Exam Guide. Columbus: McGraw-Hill Osborne.

Wärtsilä. 2016. Remote Monitoring and Assistance System (RMS). Available: http://www.wartsila.com/products/marine-oil-gas/electrical-automation/automation/remote-monitoring-and-assistance-system-rms. [Accessed: 3 December 2016].

Äijälä A. 2015. Riskit miehittämättömän aluksen operoinnissa.

SURVEY QUESTIONS AND ANSWERS POSSIBILITIES

Question	Answer
How would you evaluate your own IT-skills?	Bad/Moderate/Good/Excellent
Do you feel like you manage your every day workload with your IT-skills?	Yes/No/Not sure
Do you feel like you need more training for using computer programs?	Yes/No/Not sure
If yes, which?	Free
Who do you contact when you encouter computer related problem?	Free
Do you use cloud saving?	Yes/No/Not sure
Have you seen inside computer casing or do you otherwise know computer's structure?	Yes/No/Not sure
Have you ever installed an operating system?	Yes/No/Not sure
Do you know where to find computer's IP-address?	Yes/No/Not sure
Have you ever used any of the following tools: device manager, disk management, Regedit?	Yes/No/Not sure
Do you have an IT-related degree?	Yes/No
If yes, which?	Free
Have you been in IT-related courses?	Yes/No
If yes, which?	Free
Do you have virus protection installed on your personal computer?	Yes/No/Not sure
Does anti-virus software give protection from all threats?	Yes/No/Not sure
How often do you scan your computer for viruses?	Once in 2 weeks/Once a month/Once in 3 months/less frequently
Do you scan downloaded files for viruses before opening them?	Yes/No/Not sure

Does your password include following: small and capital letters, numbers, special signs?	1/2/All
Do you have backups of your own files?	Yes/No/Not sure
Is it safe to plug your own usb-stick to ship's computers?	Yes/No/Not sure
Do you open attached files in messages from unknown sender?	Yes/No/Not sure
How many different passwords do you have in your personal use?	1/2/3/More
Do you take action if password have leaked from services you use?	Yes/No/Not sure
Are smartphones and tables safe from viruses and malware?	Yes/No/Not sure
Have you ever configured a firewall?	Yes/No/Not sure

CONSILIUM ECDIS TECHNICAL SPECIFICATIONS

CONSILIUM ECDIS

Technical Specifications

Monitor

Display	19" LCD TFT, 23" LCD TFT, 27" LCD TFT
Resolution	1280x1024, 1600X1200, 1920x1200
Viewable angle	+/- 85 deg. (typical) (up/Down/Left/Right)
Max colours	16.7 millions (depending on graphics card)
Light Intensity	250 cd/m² (typical)
Contrast Ratio	500:1 (typical)
Dimming Range	0-100%
Active Display Area	408.0 mm (W) x 306.0 mm (H)

Computer

Processor	1 x Intel® Core™2 Duo Desktop Processor P8400 - 2.26GHz
Memory	2 x 1 GB installed (Dual Channel 200-pin DDR2 800MHz SO-DIMM)
Graphic	Intel® Graphics Media Accelerator GMA 4500MHD Integrated/Daughter Board (CH7307C)
Hard Disk	1 x Replaceable SSD 30GB or more* 2.5" SATA
Serial Com Ports	4 xs opto isolated ports 1 x MOXA Serial I/O Card (4 x COM ports - Supports RS-232/422/485) 1 x RS-232 (COM1) + 1 x RS-232/RS-422/RS-485 (COM2)
USB Ports	4 x USB ports - Supports 2.0 & 1.1
Ethernet 1	1 x 10/100/1000Mbps, ICH9M Intel® 82567L 1 x RJ-45
Ethernet 2	1 x 10/100/1000Mbps, Intel® 82574L PCI-E Gigabit LAN Controller
PCI Slots	2 x PCI Rev2.3 Slot 32-bit, 3V and 5V Interface (one used Default Configuration)

Power

Power supply	115&230VAC - 50/60Hz + 24VDC Model HT B18 STD-Axxx (60W)
Power consumption	Computer operating: 30W 19" display: 100 W (max) 23" display: 95W (typ) 200W max 27" display: 200W max

Environment

Operating temperature	-15°C to +55°C
Storage temperature	-20°C to +60°C
Relative humidity	10%~95%, non-condensing

Software

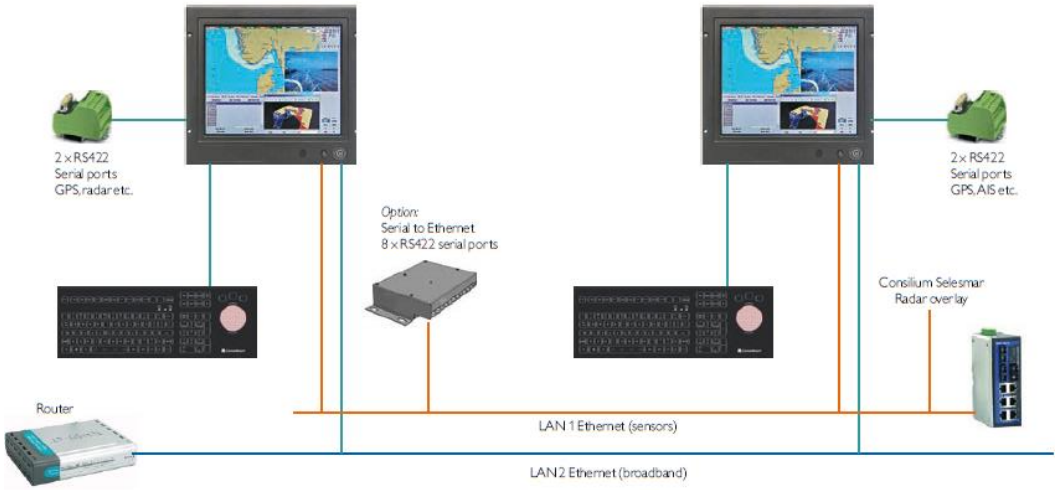
1 x Microsoft® Windows® Embedded Enterprise (XP Professional Eng w/SP2c, 32bit)
Consilium ECDIS software

Approvals

CE, Wheelmark (EU). Fully compliant with Annex A.1, item No.A ¼ and Annex B, Module B in the Directive. IMO Resolutions A.694(17), MSC 191(79) & MSC232(82).) and technical standards IEC 60945 (2002), IEC 61174 (2008), IEC 61162-1 (2007), IEC 62288 (2008)

Options/alternatives

- 19" TFT flat panel computer
- Multidisplay and Rack Computer
- ECDIS SW license only
- Radar video overlay
- Chart update service
- Weather, port, tide and current information services
- UPS
- Deck mounted console
- Extra stations



Global Service Network
Consilium Marine & Safety is represented in more than 50 countries and has a presence in the most frequently used ports around the world. Customers are able to obtain spare parts or conduct servicing via the network of subsidiaries and agents. So no matter where you are you are never far from a Consilium expert.

After sales support you can rely on
Consilium prides itself on providing customers with the benefit of a highly trained and resourceful after sales team. Each member of the team is fully experienced so customers have the added assurance of knowing that when they buy from Consilium complete customer satisfaction is an essential part of the deal.

Operator Training
Consilium offers it customers operator training courses with the focus on the safe operation of Consilium ECDIS, proper uses of various types of ECDIS related information and knowledge of the capability and limitations of electronic chart systems.

Training on demand
To help customer to get the most out of our equipment Consilium offers educational courses and training seminars from their global network of offices. So should a customer have a special requirement Consilium representatives can help arrange and conduct specific seminars where attendees can discover everything there is to know about a particular product and it's functions.